Reference Code: TA001537SEC
Publication Date: November 2008
Author: Alan Rodger

Butler Group
a Datamonitor Company

TECHNOLOGY AUDIT

Entrust TransactionGuard v3.2.1

Entrust

BUTLER GROUP VIEW

ABSTRACT

Entrust TransactionGuard is a fraud detection solution that checks all user activity around HTTP-based transactions within online systems. It is typically used by fraud administrators and analysts, and provides a centralised fraud protection service that can operate across application boundaries within the enterprise. Although essential, detecting fraud can be a costly undertaking that brings challenges relating to operational consistency and efficiency, and incorporating sufficient flexibility to meet complex and changing requirements. Entrust TransactionGuard enables organisations to deploy a range of risk-based measures to detect (and, valuably, prevent) fraud by online users, including dynamically requesting additional authentication, and recognising behavioural changes. The solution can be enabled to recognise and associate users' behaviour across application boundaries, and all but its most advanced features require no application changes. Butler Group believes TransactionGuard to be a valuable weapon against online fraud, which is exceptionally well suited to Entrust's target market of large financial institutions.

KEY FINDINGS

- ✓ Prevention, rather than solely detection, of fraud.
- ✓ Real-time, dynamic risk assessment focuses on service as well as security.
- ✓ Can initiate extra authentication if risk is identified, for added protection.
- ✓ Detection and prevention need not impact application logic.
- ✓ Powerful facilities to enable recognition of dangerous IP addresses.
- ✗ Adds an overhead to change, as any change to application message content must be reflected within TransactionGuard.

Key: ✓ Product Strength ✗ Product Weakness ⓘ Point of Information

LOOK AHEAD

Planned developments include support for the open sharing of fraud data, multi-channel fraud support (including IVR, and ATM), and evolutions in the way that fraud can be administered.

FUNCTIONALITY

Product Analysis

Entrust TransactionGuard is a real-time fraud detection solution that transparently monitors transactions and uses passive detection techniques to identify fraudulent activity. It uses advanced behavioural understanding of transaction patterns, and in-depth user profiling, and is comprised of three core components (see Figure 1) – Real Time Fraud Detection (RTFD), FraudMart, and the Open Fraud Intelligence Network (OFIN).

Most fraud detection solutions rely on one of two discrete approaches: to compare the time of the day of user login with norms for that person, or 'instrumenting' applications themselves (i.e. incorporating code at key functional points to reveal key data). The first has only minimal value, as there are far more behaviour factors that should be taken into account, and the weaknesses of the second approach include the difficulty of responding to change, and the limitation of requiring data analysis (likely to be manual) to determine that action is necessary.

Entrust TransactionGuard is different in many ways to most competing solutions, primarily in the sense that customers do not have to modify applications to undertake fraud monitoring. The Entrust solution is 'trained' by fraud analysts within the customer organisation to recognise how HTTP messages make up the organisation's application traffic, so that during live operation it can recognise what users are doing in business terms, without integrating with applications themselves. Once 'trained', TransactionGuard automatically implements the many built-in rules that are supplied for identifying fraud behaviour, against the applications. Indeed, it can also monitor sequences of transactions across application boundaries – a highly important capability, as understanding the totality of several user actions can be as important as the significance of any single user interaction. For example, if a user modifies an address first, then makes a financial amendment, this could indicate an attempt to compromise a system by a user who is looking to gain advantage quickly.

The ability to understand the significance of transaction sequences is built up using a notable capability within the solution, that enables a fraud analyst to undertake a virtual walk-through of the transactions within an application, while TransactionGuard gathers details of the HTTP traffic relating to each transaction. The monitoring of HTTP traffic during live operation by the RTFD Passive Listener is then analysed by the Fraud Detection server in terms of application transactions, enabling a picture to be built up of application signatures, and sequential activity that might indicate fraudulent activity. It is important to consider the overhead factor that this approach introduces, namely that any program changes that affect application message content should be reflected via the fraud analyst 're-recording' the transactions so that new message formats can continue to be recognised as transactions.

RTFD identifies 'normal' patterns of behaviour via a rule-based approach, which reduce false positives compared with other methods of decision making over the short term. Factors such as the user's location, the time of day, and function usage pattern are individually assessed by user-configured rules which build up a risk score, and TransactionGuard then allows application logic to decide what action is appropriate (e.g. stop a transaction based on potential fraud, or contact with the customer to discuss the circumstances).

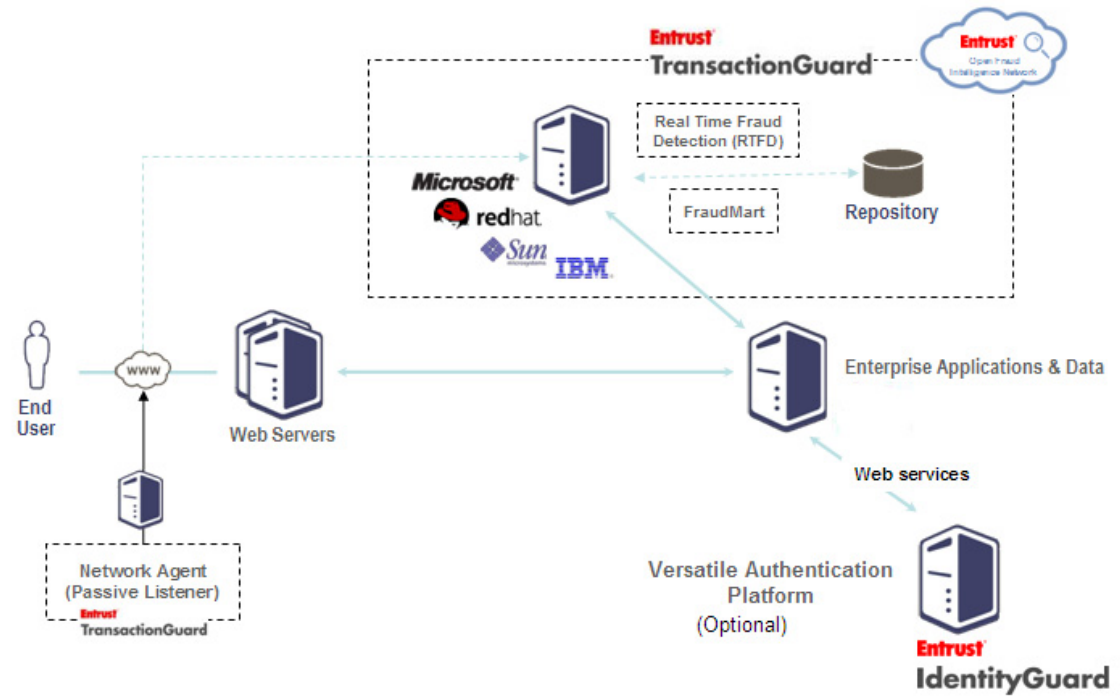
TransactionGuard forms one of the core components of Entrust's Identity and Access Management (IAM) technology platform, and can enable applications to invoke extra user authentication (if that is an appropriate action) via integration with Entrust IdentityGuard. Such circumstances typically include invocation of additional authentication checks due to risk- and situation-specific reasons. In such an approach all operational control remains with the application in order to ensure continuity of look and feel.

Customers using Entrust IdentityGuard may also take advantage of its integration with the Acxiom product FactCheck-X: Authenticate, to enhance identity proofing via detailed question and answer responses. This uses demographic and geographic data in challenge questions, with nearly 900 data elements for more than 300 million individuals, and compares transaction details with over 25 US and international watch lists.

All captured transaction details, risk events, and internal TransactionGuard data such as rules, are stored in the solution's repository. The solution's FraudMart component provides forensics and data querying, in order that past incidents can be investigated, and reports specified. Also TransactionGuard provides facilities to assign fraud instances to different analysts, via workflow, and can transfer case management notes alongside.

OFIN is an information sharing service designed to help combat online fraud by consolidating and sharing data on important fraud behaviour patterns. The facility provides participating members with the latest fraud information as it becomes available. The service consolidates information from a variety of sources, including leading financial organisations, IP geo-location information, anonymous and open proxy data, and host reputation scores. Organisations can use OFIN to readily adapt to new fraud patterns found in the wider world, as Fraud Administrators can download details from OFIN's news site, which incorporate suggested new rules. While rules can be downloaded, they would require customisation by each organisation in terms of application interface, and action requirements.

Figure 1: Entrust TransactionGuard Architecture Overview



Source: Entrust

DATAMONITOR

Product Operation

TransactionGuard builds two types of risk score that are relevant to each transaction. Session Risk Scores take into account factors such as user location, transaction sequence, and transaction amounts. User risk is the other type, compiled by comparing the user's behaviours in the current session with the normal customer profile for that user that TransactionGuard builds up over time.

The Passive Listener is sited in front of the Web server, and gathers HTTP transaction details. The profiling by RTFD takes the following transaction characteristics into account:

- Device profile – RTFD recognises the use of unique devices (and their human users) across multiple sessions. By including the ID of historical devices used as a part of user data, it can factor risk arising from any change of device being used by a given user.
- IP address, which is checked against a blacklist of IP addresses that are known to be compromised, and against a whitelist (detailing domains that are known to be credible, such as AOL addresses).
- Transaction sequence, which is discerned by tracking specific user activities in an application, identified by using the data available in the HTTP stream (e.g. service path, query string, cookies, post data, response body, etc.).
- Transaction attributes, which are assessed against the fraud detection rules.
- Real-time host reputation data from OFIN.

OFIN provides two levels of service, each of which makes different data available to the customer organisation:

- Standard Version, which allows for location vetting by providing IP-Geolocation – comprehensive information about IPs on the Internet, including satellite, proxies, and anonymous proxies.
- Advanced Version, which enables assessment of the reputation of an IP address ("Host Reputation") based on a real-time data feed. Host reputations are calculated based on over 130,000 submission sources on the Internet.

The rules with which TransactionGuard assesses transaction activity, and builds up session and user profiles, can be fully customised. Data attributes and rule conditions are evaluated by RTFD, which sets risk scores resulting from each rule, these combining to be attributed as an overall score and assessed as to whether activity is suspicious, and what action is required. User activity is profiled over time, to better understand anomalies and potential fraud. Fraud analysts can use facilities to view in real time the users and/or sessions with the most suspicious activity alerts, and alerts can be assigned to specific fraud managers for further analysis.

With the optional integration available with Entrust IdentityGuard, an application can call TransactionGuard and IdentityGuard via Web services protocols, and Entrust authentication logic is available as if it were embedded within the application. User and session risk scores are available to all functionality in real time, and can be used to determine if second-factor authentication should be initiated. This action is usually taken at login time according to risk scores, although an application can use the functionality to demand additional authentication during a transaction or sequence (for example, if suspicious activity becomes evident, or if a suspiciously large transaction amount is suddenly a factor). A number of decision factors are typically employed, including:

- Whether the user is situated at the expected client machine, or if not whether Geo-IP City, Country, Timezone ,or ISP are also new for the user.
- Whether the IP Address Geo-IP City/Country are blacklisted, or the IP Address has a bad Host Reputation score, or has been used for multiple logins by different users within the last few hours.

Product Emphasis

TransactionGuard provides centralised fraud detection across business application boundaries, hence enabling improved consistency and efficiency over application-specific approaches. Furthermore, easier maintenance of fraud policy, and broader policy enforcement is also a significant benefit. Especially when dealing with Internet-based transactions, responsiveness is critical, and TransactionGuard gives organisations the opportunity to control transaction checks and protection in real time, based on the real-time, dynamic risk score.

When compared with the traditional approaches of leveraging batch reports and working those reports days later, use of Entrust TransactionGuard for real-time fraud detection means that fraud can be avoided or stopped before any financial impact hits the organisation. Risk and doubt over identity and access rights within an organisation's customer-facing applications are strongly addressed – the use of the real-time risk score in conjunction with increased authentication strength, all under the application's control, delivers assurance that the right end user is actually the transaction subject.

DEPLOYMENT

Entrust recommends its own Professional Services organisation to deploy Entrust TransactionGuard, as high-end skills in security, networking, and large-scale architectures (as well as product knowledge) are commonly necessary in order to handle potential complexity. A 12-14 week deployment effort is typical, spanning the initial requirements analysis activities through to live operation. Entrust positions the implementation approach as low risk, with minimal impact to the existing operational implementation, due to there being no need to modify a customer's applications. Entrust resources' deployment involvement typically includes installation, configuration, fraud rule tuning, live deployment, and operational training.

Capabilities can be adopted incrementally – e.g. integration with Acxiom or Entrust IdentityGuard could be added after an initial implementation, and of course additional and modified rules can be incorporated at any time within the fraud protection deployed. From an architectural perspective, the solution can be deployed across multiple machines and physical locations. Post-deployment, the extent of management overhead is characterised by Entrust as being typical for a back-end application, requiring time from administrators to maintain hardware, application servers, and operating systems. The potential for greater productivity for fraud analysts should certainly mean at least that no additional users would need to be assigned. On-site training is provided by Entrust as part of every deployment, both to the customer's technical team supporting the product, and (separately) to the customer's fraud analyst team.

The passive listening component (a network agent) is a stand-alone appliance. The Entrust TransactionGuard server software can be run on AIX 5.3, RedHat Linux 3.0 & 4.0, Solaris 10, or Windows Server 2003, and requires an Oracle 10gR2 database which is licensed separately by the customer. OFIN is a hosted service operated by Entrust, available via a Web services interface.

The solution's primary approach to transaction monitoring is via the HTTP traffic stream, but it can be configured and deployed using custom adapters for listening to transactions from legacy systems, broadening fraud protection within the customer organisation. Fraud management business processes are likely to change considerably to take advantage of the solution, and although no application changes are essential, features such as using risk scores to change customer authentication requirements have to be handled within applications, and so would require applications to be changed.

The specific licensed components of the solution are:

- Entrust TransactionGuard Device Profiling.
- Entrust TransactionGuard RTFD (Real time Fraud Detection).
- Entrust TransactionGuard FraudMart.
- Entrust Open Fraud Intelligence Network.

Every deployment of Entrust TransactionGuard includes the Real-time Fraud Detection component (which includes transaction monitoring via the network agent for passive listening). For device profiling, this is a licence-restricted option that delivers sophisticated device profiling for organisations with singular requirements of this type. Optional components are Entrust TransactionGuard FraudMart, and the Entrust Open Fraud Intelligence Network service. Pricing for the solution is on a per user basis. Support is provided via Entrust's global, 24x7 support capability.

PRODUCT STRATEGY

TransactionGuard is primarily targeted at financial institutions, owing to the focus of its core fraud detection capabilities – the top 500 global financial institutions are the main target market. The key opportunity Entrust foresees is the ability to address additional channels such as Interactive Voice Response (IVR) systems, and Automated Teller Machine (ATM) systems, with a single solution in a way that is non-intrusive and accommodates evolutionary change.

Entrust has relationships with several global partners including BT, Symantec, and CAC (from Japan) to sell and support the solution, which is also sold direct. It is supported by technology partnerships with Oracle and Red Hat. The solution is sold on a perpetual or subscription basis – the support model for the perpetual option is on a per-user plus basis, which can be annualised to provide pricing flexibility. Entrust states that initial implementations typically have six-figure costs, and that 70% of these costs would commonly be attributable to software, and 30% to services. Entrust has a support fee scheme in which predefined levels are provided for fixed proportions of the initial software costs – Silver (18%), Gold (20%), and Platinum (22%). Entrust plans one major release every 14-18 months, with interim smaller releases or service packs as appropriate. Planned developments include support for the open sharing of fraud data (as per an Information Engineering Task Force standard which Entrust is helping to steer), multi-channel fraud support (including IVR, and ATM), and evolutions in the way that fraud can be administered.

Entrust TransactionGuard is not so much a discrete solution as a strong enabling capability, providing organisations with on-premise fraud detection facilities that process end-user transaction data on site, avoiding the need to forward sensitive information off site for fraud analysis. Return on Investment (ROI) arises from a large number of quantifiable sources such as reductions in losses due to fraud, improved fraud analyst productivity, reduced costs of fraud monitoring, reduced capital cost of providing broader fraud coverage, and elimination of legal costs of pursuit of fraud perpetrators.

COMPANY PROFILE

Entrust is a publicly traded company (NASDAQ: ENTU) with headquarters in Dallas, Texas, in the US and other major offices in Washington DC, San Francisco, Ottawa, and London. Entrust began its life in 1994 as a division of Nortel Networks, operating as Nortel Secure Networks where it was responsible for significant pioneering work on Public Key Infrastructure (PKI), a technology area where it continues to be positioned as a market leader. In 1996, the company spun away from Nortel and today sells layered security solutions under three broad portfolio headings: PKI, Information Protection, and Risk-based Authentication (authentication coupled with fraud detection). In mid-2006 Entrust acquired a company called Business Signatures, and with it the product that is now called Entrust TransactionGuard.

Entrust currently employs around 450 staff across its operations, the breakdown being 300 in Canada, 70 in the US, and the remainder spread across its European and rest-of-the-world operations. Its total customer base has grown to in excess of 1,700 companies in 50 different countries. Entrust has not provided statistics relating to customers for TransactionGuard specifically, but does state that the insurer United Services Automobile Association, and a US bank, each have implementations that deal with around five million users.

Almost half of the company's recent revenues have arisen from business in the US, as well as 21% from business in Canada (the rest being from Europe and Asia). Table 1 shows a summary of the company's financial position as reported at the end of its three most recently completed financial years:

Table 1: Financial Details

Year ending 31 December	2007	2006	2005
Revenue (US$ Million)	99.7	95.2	98.1
Gross Profit (US$ Million)	60.1	57.2	61.7
Total Net Income/(Loss) (US$ Million)	(6.2)	(15.4)	6.4

Source: Entrust DATAMONITOR

SUMMARY

Entrust TransactionGuard is a very powerful tool with which to counter fraud perpetrated within online applications. Its highly flexible, configurable, rule-driven analysis provides real-time responsiveness based in risk scoring of activity, taking into account the characteristics of both the user, and the entire online session. It is able to take into account the totality of potentially fraudulent activity regardless of the boundaries of individual applications, this being representative of the business-oriented focus that pervades throughout the solution.

Butler Group believes this to be a highly valuable solution for organisations in Entrust's target market – specifically, those with most to lose from failing to respond to risk in the same short timeframe as malevolent users in an online environment can hit the company's bottom line.

Table 2: Contact Details

Entrust Worldwide Headquarters
One Hanover Park
16633 Dallas Parkway
Suite 800
Addison
75001 Texas
USA
Tel: +1 (888)690 2424
Fax: +1 (972)713 5805
E-mail: entrust@entrust.com
www.entrust.com

Entrust EMEA Headquarters
Apex Plaza – B2
Forbury Road
Reading
Berkshire
RG1 1AX
UK
Tel: +44 (0)118 953 3000
Fax: +44 (0)118 953 3001
E-mail: emea.sales@entrust.com

Source: Entrust

DATAMONITOR

Headquarters
Shirethorn House,
37/43 Prospect Street,
Kingston upon Hull,
HU2 8PX, UK
Tel: +44 (0)1482 586149
Fax: +44 (0)1482 323577

Butler Direct Pty Ltd.
Level 46, Citigroup Building,
2 Park Street, Sydney,
NSW, 2000,
Australia
Tel: + 61 (02) 8705 6960
Fax: + 61 (02) 8705 6961

Butler Group
245 Fifth Avenue,
4th Floor, New York,
NY 10016,
USA
Tel: +1 212 652 5302
Fax: +1 212 202 4684